Gebruik OpenAPI om informatie over ISE-certificaten op te halen op ISE 3.3

Inhoud

Inleiding

Dit document beschrijft de procedure voor het gebruik van openAPI om het Cisco Identity Services Engine (ISE)-certificaat te beheren.

Achtergrond

Geconfronteerd met toenemende complexiteit op het gebied van netwerkbeveiliging en -beheer voor ondernemingen, introduceert Cisco ISE 3.1 OpenAPI-geformatteerde API's die het beheer van de levenscyclus van certificaten stroomlijnen, en een gestandaardiseerde en geautomatiseerde interface bieden voor efficiënte en veilige certificaatbewerkingen, waardoor beheerders sterke beveiligingsprocedures kunnen afdwingen en netwerknaleving kunnen handhaven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Identity Services Engine (ISE)
- REST API

- Python

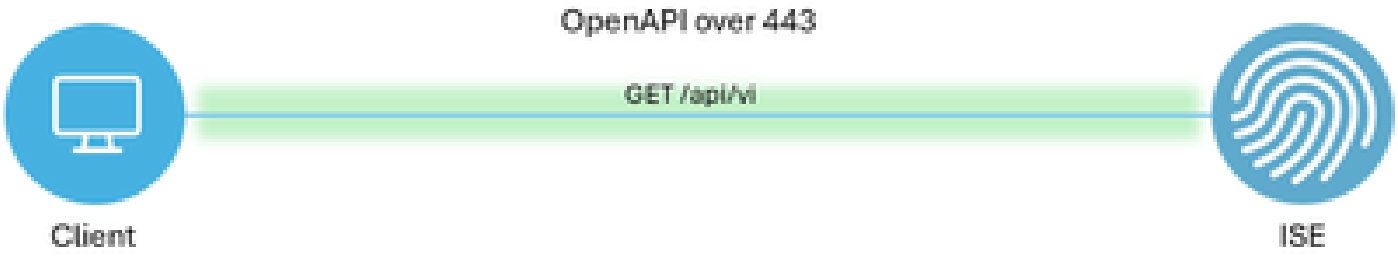
Gebruikte componenten

- ISE-lijnkaart 3.3
- Python 3.10.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram

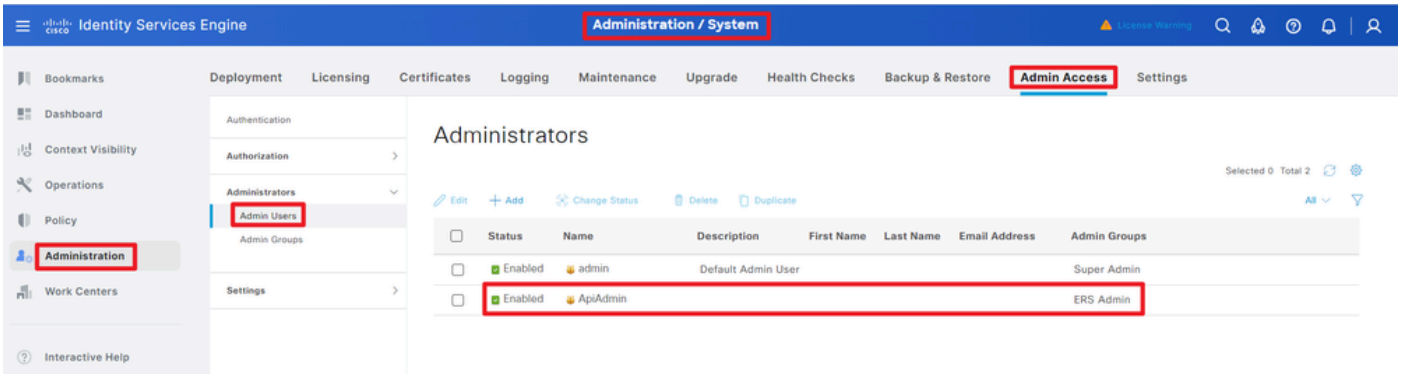


Topologie

Configuratie op ISE

Stap 1: Voeg een Open API Admin account toe

Om een API-beheerder toe te voegen, navigeer naar Beheer > Systeem > Admin Access > Beheerders > Admin Gebruikers > Add.

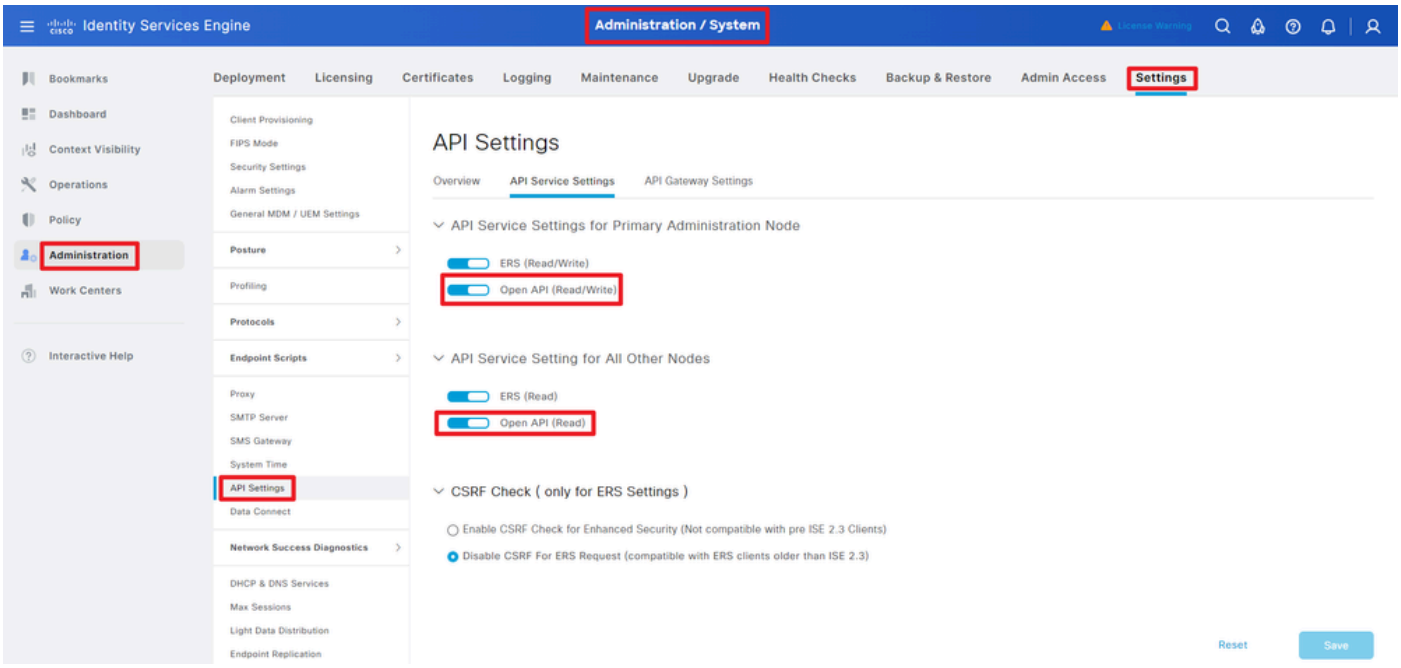


API-beheerder

Stap 2: Open API inschakelen op ISE

Open API is standaard uitgeschakeld op ISE. Om het in te schakelen, navigeer naar Beheer > Systeem > Instellingen > API-instellingen > API-serviceinstellingen. Schakel de opties voor Open

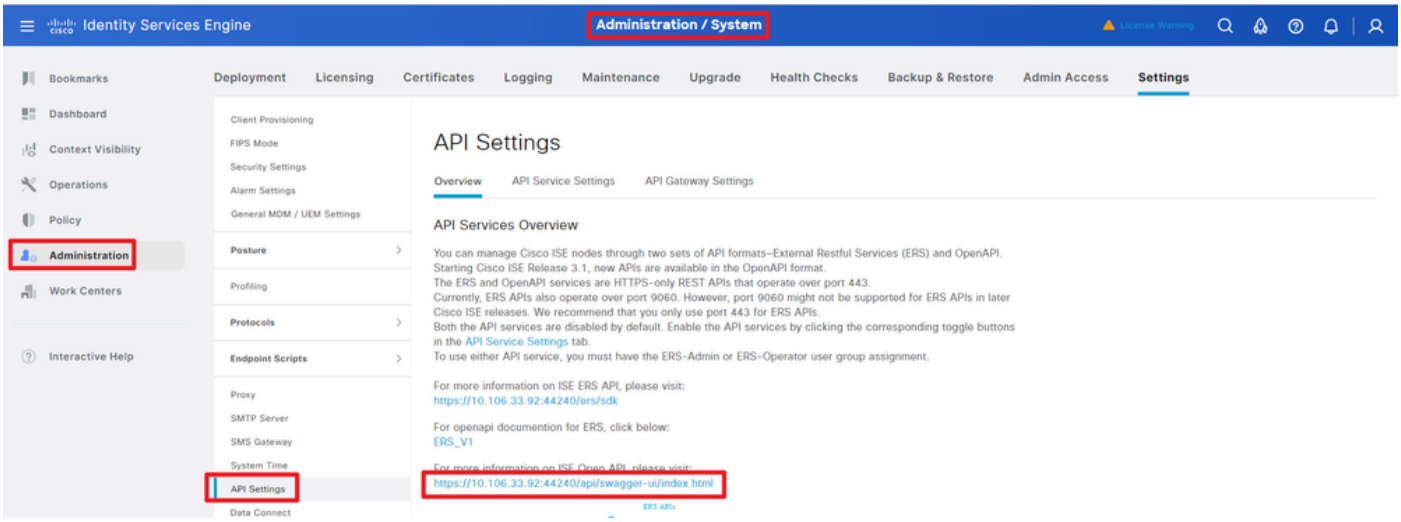
API in. Klik op Save (Opslaan).



OpenAPI inschakelen

Stap 3: Verken de open API van ISE

Ga naar Beheer > Systeem > Instellingen > API-instellingen > Overzicht. Klik op Open API bezoek link.



Bezoek OpenAPI

Python-voorbeelden

Ontvang alle systeemcertificaten van een bepaald knooppunt

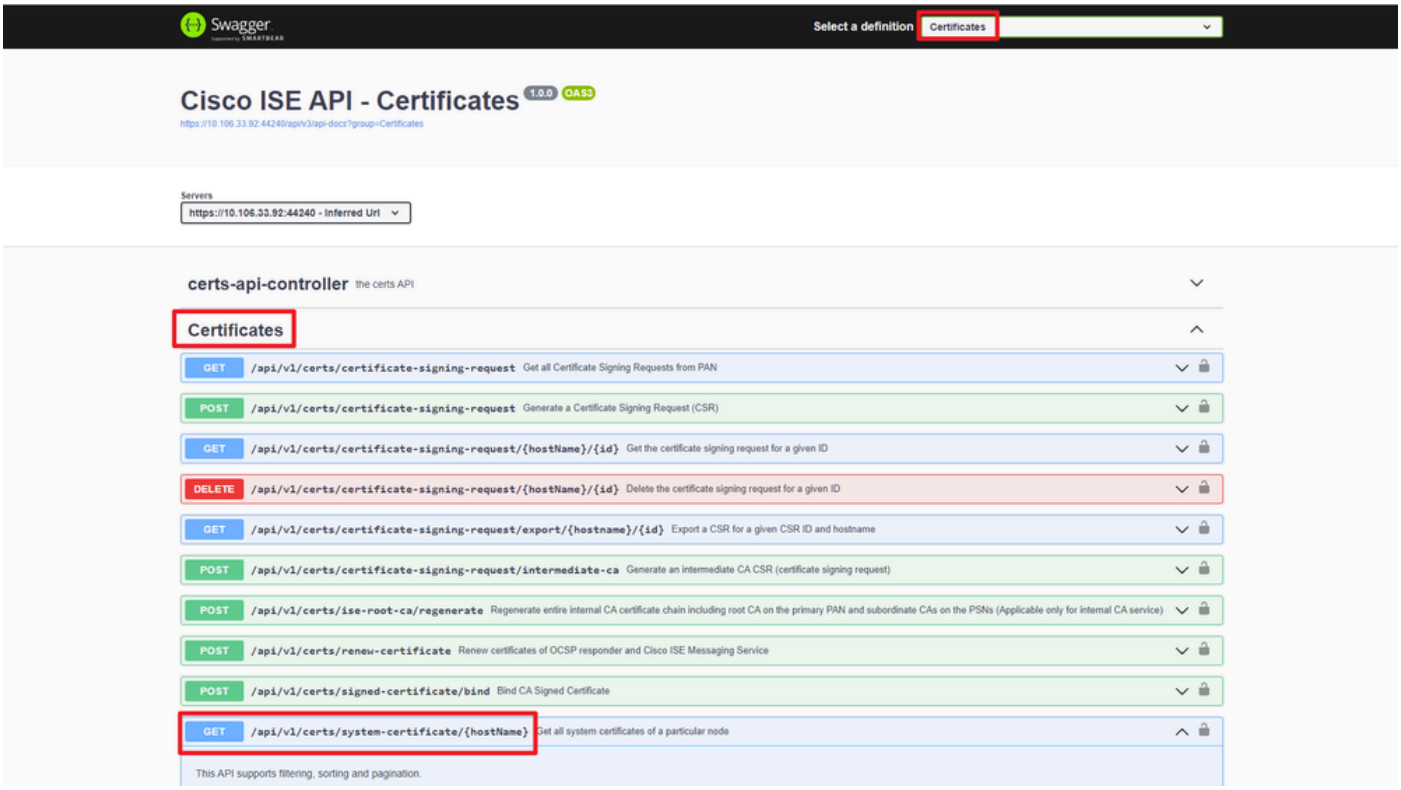
De API geeft een lijst van alle certificaten van een bepaald ISE-knooppunt.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN

URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om certificaten van een bepaalde ISE-knooppunt op te halen.



API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

<#root>

```
from requests.auth import HTTPBasicAuth
import requests

requests.packages.urllib3.disable_warnings()

if __name__ == "__main__":

    url = "
```

https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN

```
"
    headers = {
"Accept": "application/json", "Content-Type": "application/json"
}
    basicAuth = HTTPBasicAuth(
"ApiAdmin", "Admin123"
)
    response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
    print("Return Code:")
    print(response.status_code)
    print("Expected Outputs:")
    print(response.json())
```

Hier is het voorbeeld van de verwachte outputs.

```
Return Code:
200
Expected Outputs:
{'response': [{'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME0
```

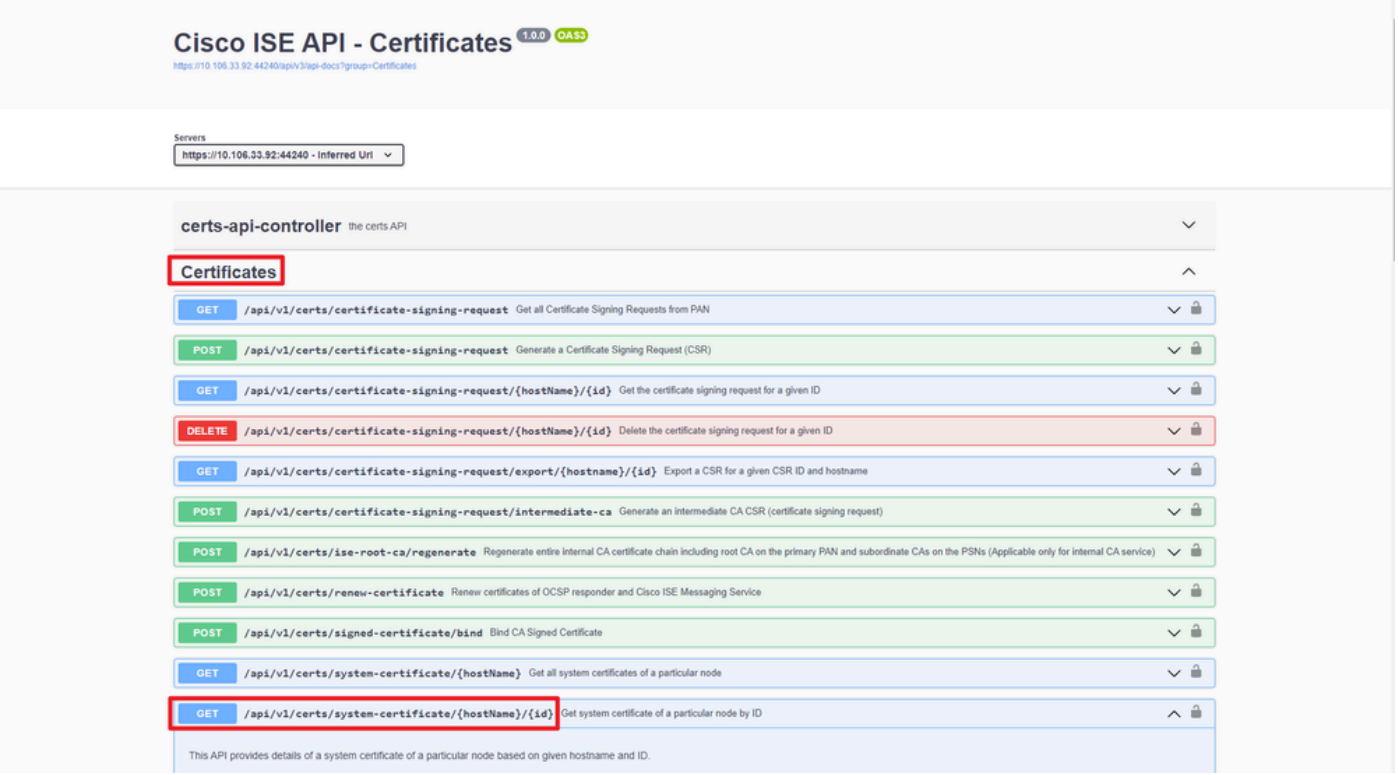
Systeemcertificaat van een bepaald knooppunt verkrijgen via ID

Deze API geeft details van een systeemcertificaat van een bepaald knooppunt op basis van een gegeven hostnaam en ID.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-of-Certificate>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om het certificaat van een bepaald knooppunt op te halen op basis van de gegeven hostnaam en ID.



API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN/5b5b28e4-2a51-495c-8413-610190e1

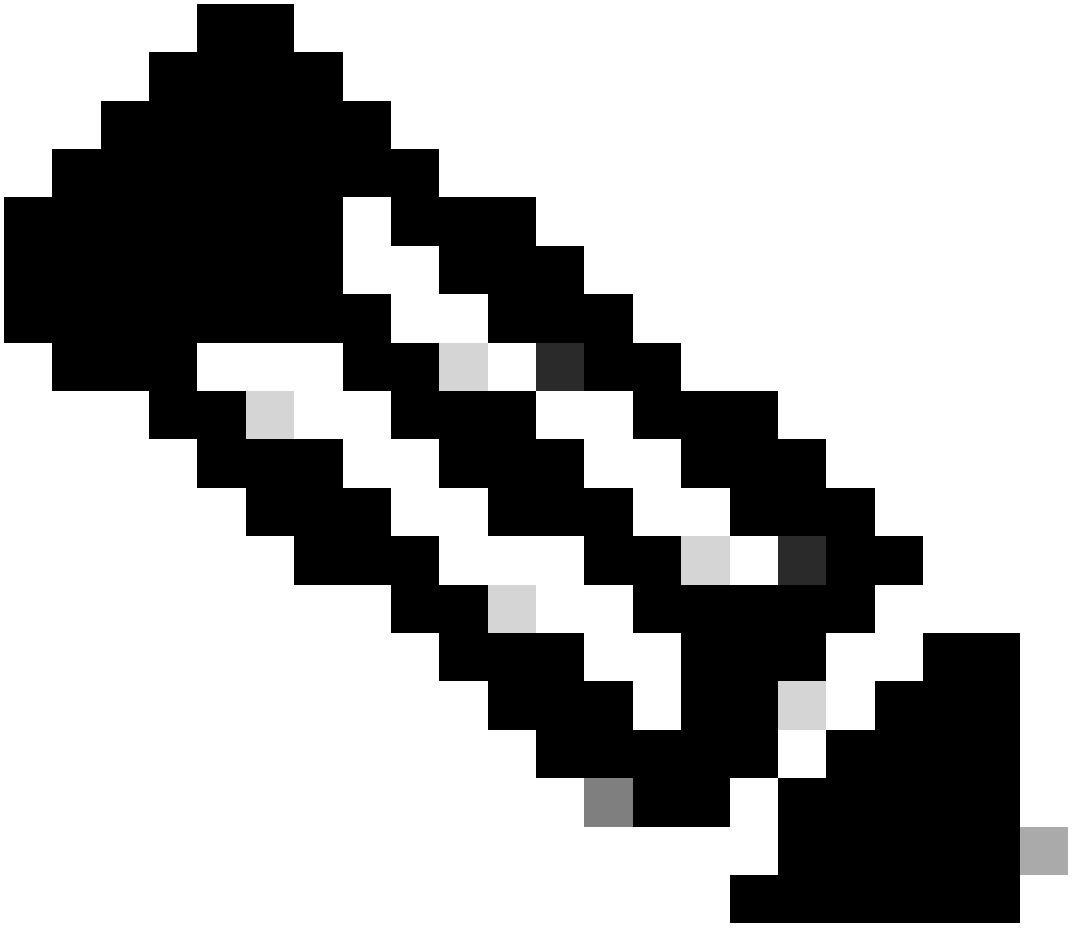
" headers = {

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")



Opmerking: de ID is afkomstig van API-uitgangen in stap 3 van "Get All System Certificates Of A Particular Node", bijvoorbeeld, 5b5b28e4-2a51-495c-8413-610190e1070b is "Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com".

Hier is het voorbeeld van de verwachte outputs.

Return Code:
200
Expected Outputs:
{'response': {'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02

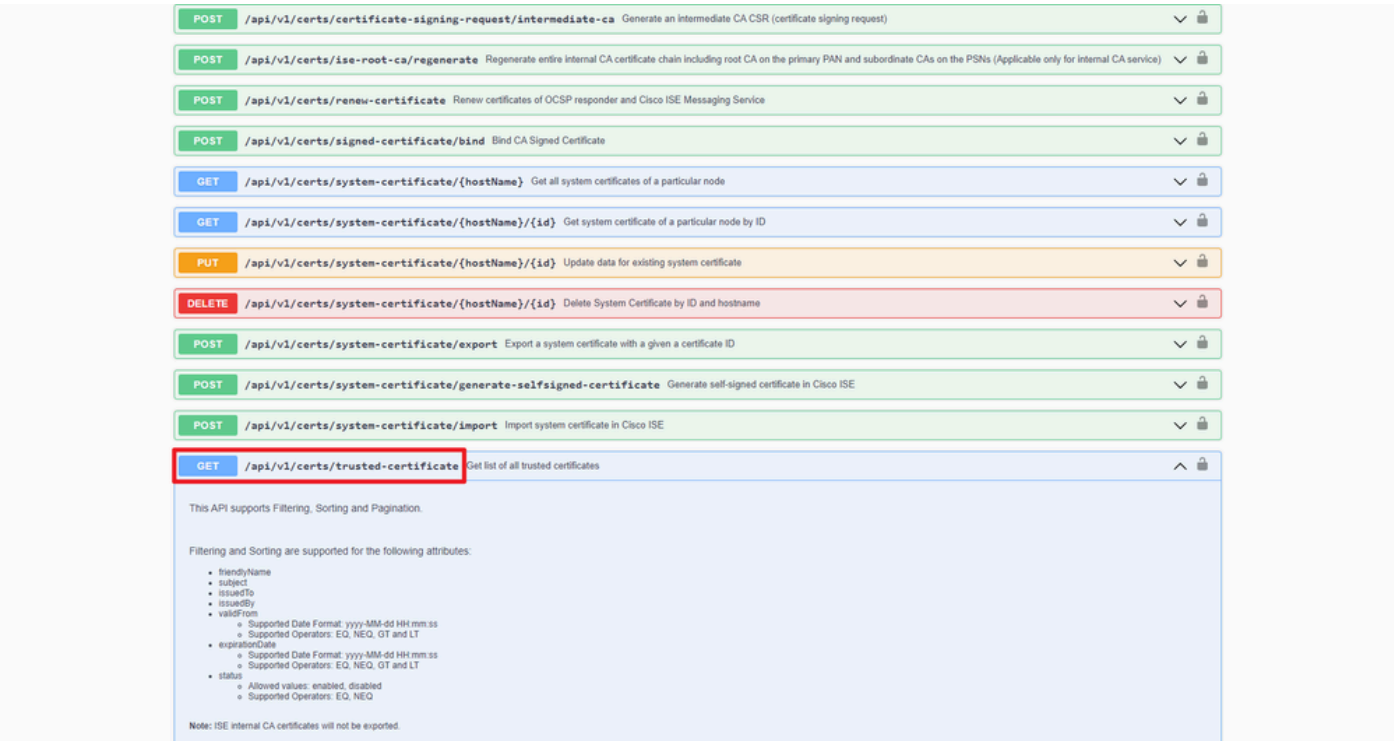
Een lijst met alle vertrouwde certificaten opvragen

De API maakt een lijst van alle vertrouwde certificaten van ISE-cluster.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/certs/Trusted-certificate
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om vertrouwde certificaten op te halen.



API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/trusted-certificate

" headers = {

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

```
"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")
```

Hier is het voorbeeld van de verwachte output.(weggelaten)

```
Return Code:
200
Expected Outputs:
{'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=Ver
```

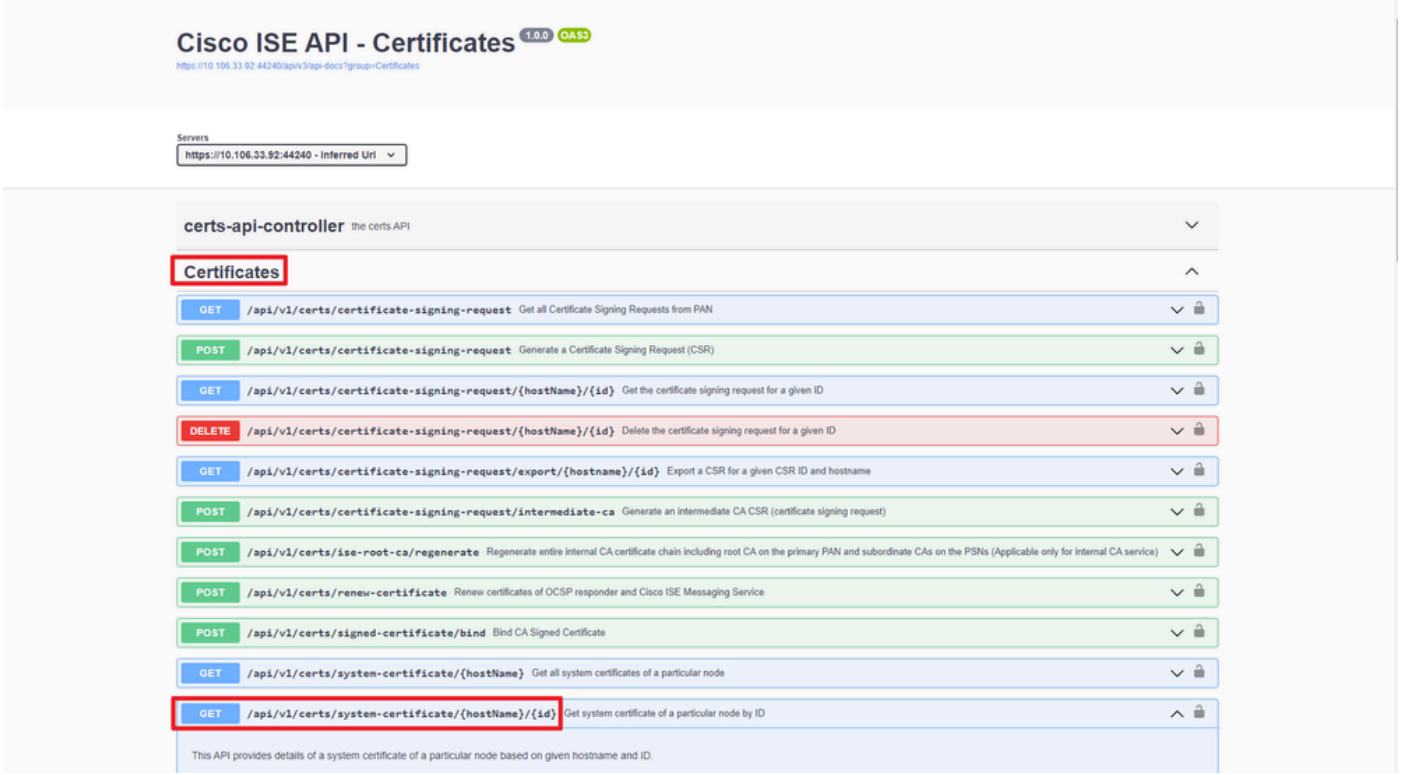
Vertrouwenscertificaat per ID verkrijgen

Deze API kan details van een vertrouwenscertificaat weergeven op basis van een gegeven ID.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/certs/Trusted-certificate/<ID-of-Certificate>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om implementatieinformatie op te halen.



API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

<#root>

from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "

https://10.106.33.92/api/v1/certs/trusted-certificate/147d97cc-6ce9-43d7-9928-8cd0fa83e140

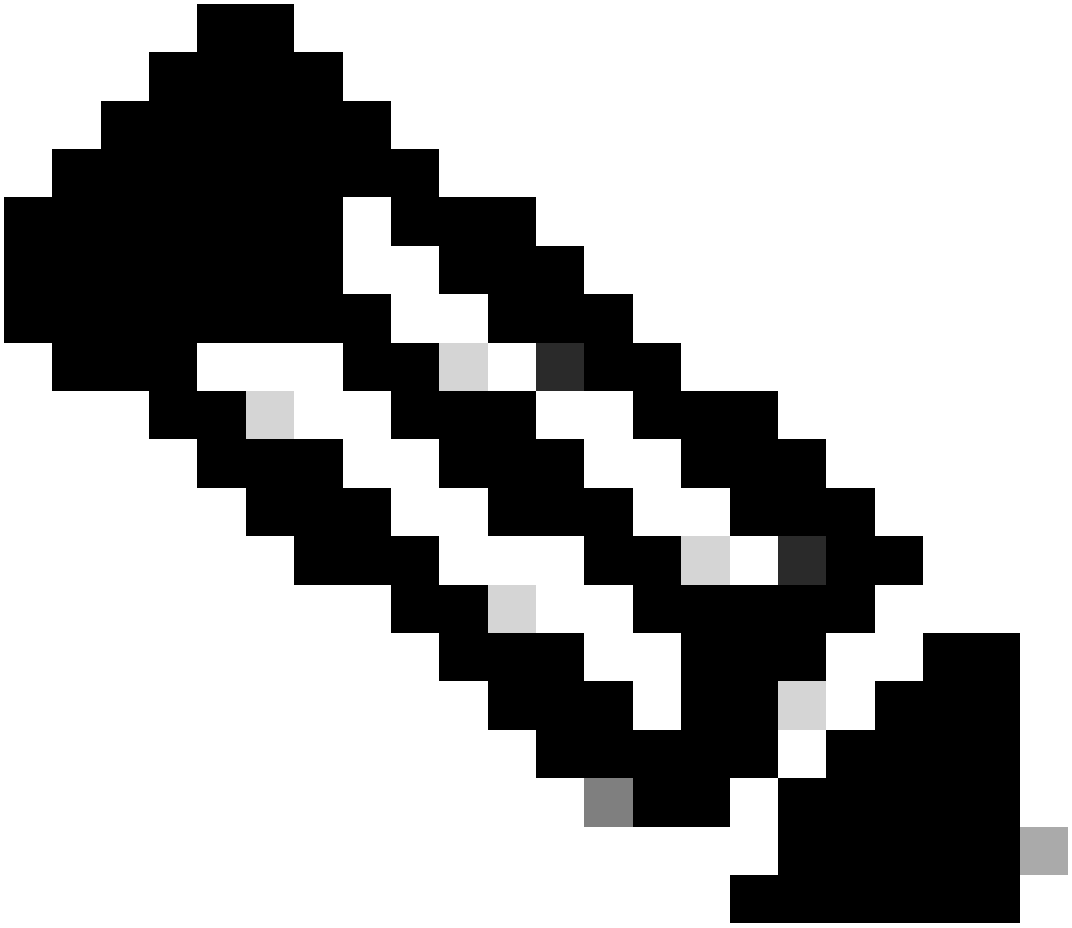
" headers = {

"Accept": "application/json", "Content-Type": "application/json"

} basicAuth = HTTPBasicAuth(

"ApiAdmin", "Admin123"

) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")



Opmerking: De ID is afkomstig van API-uitgangen in stap 3 van "Get List Of All Trusted Certificates", bijvoorbeeld, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 is "VeriSign Class 3 Public Primary Certification Authority".

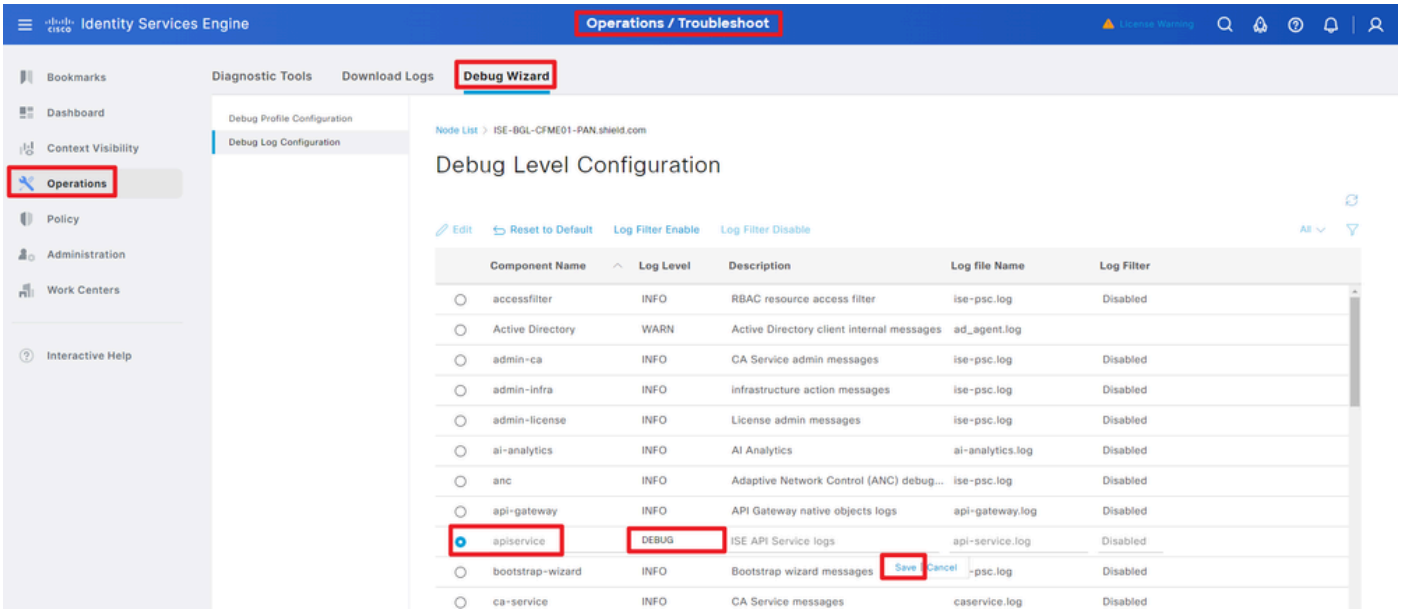
Hier is het voorbeeld van de verwachte outputs.

Return Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certifi

Problemen oplossen

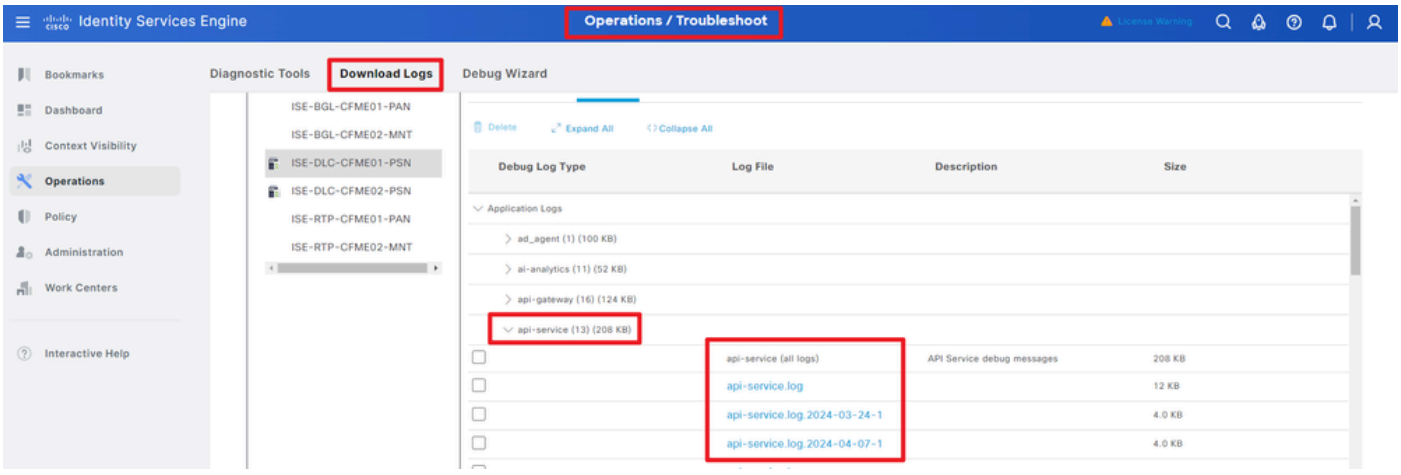
Om problemen op te lossen die betrekking hebben op de Open API's, stelt u **het** niveau **Log** voor deapiservice component in op DEBUG in **het** venster **Debug Log** Configuration.

Om debug in te schakelen, navigeer naar **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > Appliance.**



Debug van API-service

Als u debug-logbestanden wilt downloaden, navigeert u naar **Operations > Probleemoplossing > Downloadlogs > ISE PAN-knooppunt > Debug-logbestanden.**



Debug logs downloaden

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.